

# Bootstrapping Security in Personal Area Networks

Jihoon Cho

Information Security Group, Royal Holloway University of London  
Egham, Surrey, TW20 0EX, United Kingdom  
*Jihoon.Cho@rhul.ac.uk*

**Abstract:** Providing key pre-distribution in personal area networks (PANs) remains a challenging problem, in particular because of the unique characteristics of, and constraints on, such networks. Several key pre-distribution schemes have been proposed for use in PANs, but these schemes only support key management within a PAN. In a ubiquitous environment, however, users with multiple personal wireless devices are likely to form mobile ad hoc networks, requiring key management between PANs. Moreover, PANs cannot rely on the universal accessibility of an online trusted third party, and PAN users are unlikely to delegate security operations to an external trusted party for privacy reasons. We thus propose a provably secure self-organising key pre-distribution scheme for use both within and between PANs.

**Keywords:** PAN, threshold scheme, key pre-distribution

## 1. Introduction

A PAN, or Personal Area Network, is a small wireless network that covers only a personal work space, e.g. an office or a meeting room. A PAN only includes those components owned and controlled by a single user, and the components directly communicating with each other via a local interface such as Bluetooth or IrDA. Possible deployment scenarios for PANs include a smart office, a smart home, conference halls, hospitals, public areas, etc. These applications not only involve interactions within a PAN (intra-PAN communication), but also between two or more PANs (inter-PAN communication).

A range of personal wireless-enabled devices, including various types of smart phone, are now being introduced, capable of inter-communicating using multi-hop routing protocols. Wireless mesh networks (WMNs) [4] are expected to address the range limitations and to significantly improve the performance of wireless ad hoc networks and PANs. Moreover, users with multiple personal wireless devices are likely to form mobile ad hoc networks (MANETs) to transparently and securely exchange data in a ubiquitous environment. Thus, in the very near future, inter-PAN communications will potentially become widespread, where personal wireless devices such as PDAs or laptop PCs communicate with devices belonging to other PANs<sup>1</sup>. Therefore, security provisions for inter-PAN communications are becoming increasingly important.

Many security frameworks supporting key management rely on trusted third parties (TTPs), e.g. to act as key distribution centres or Certification Authorities. However, PANs, like

MANETs, cannot rely on the universal accessibility of an online TTP, because of the limited communications capacity of personal wireless devices. Moreover, PAN users are unlikely to delegate security operations to an external trusted party for privacy reasons. This clearly makes devising security solutions for PANs a challenging task. Therefore, a key management service for PANs needs to be provided in a distributed fashion, so that participating PAN users share the key management responsibility by distributing trust to a set of nodes from each PAN.

This paper has three main contributions. First, inspired by a number of key pre-distribution schemes for use in ad hoc networks (see, for example, [17], [26]), we propose a novel self-organising key pre-distribution scheme for use both within and between PANs, which does not rely on online TTPs. Second, unlike previously proposed self-organising key pre-distribution schemes for MANETs that assume *a priori* secure channels between all participating nodes, which potentially reduce the practicability of such solutions, the new scheme makes minimal use of such channels. Finally, the proposed scheme enables any pair of network nodes to establish a shared secret in a non-interactive fashion, potentially increasing the efficiency of secure ad hoc routing protocols.

The rest of the paper is organised as follows. We first give a brief definition of PANs in section 2. In the following sections, we discuss motivations and then introduce our novel key pre-distribution scheme for intra/inter-PAN communication. In sections 5 and 6, we provide the security and efficiency analysis and then discuss related issues of the proposed scheme. In section 7, we briefly discuss secure data communication in PANs based on the TLS protocol, which may use the result of our proposed scheme. Finally, we discuss related key pre-distribution schemes for use in MANETs and discuss certain security issues and limitations of these schemes.

## 2. WAN, LAN, and PAN

PANs, like other networks, can be defined in terms of distance, bandwidth, and usage. In terms of distance, LAN is generally considered to be a distance group, such as the offices of a small company or a single building of large company, and WAN refers to a large area of service, such as a corporate campus or a set of office buildings scattered around a community. At present, the term PAN exclusively refers to wireless network using communications, both radio and optical, and is usually considered to have a range of 10 metres, covering a modest

<sup>1</sup> Existing research in this area includes the work of the PACWOMAN project (<http://www.imec.be/pacwoman>).

room-sized individual work area or work group. With regard to bandwidth or data rate, PANs generally include lower data transmission systems such as Bluetooth. Of course, however, there are very high-rate systems for PANs such as Ultra-Wideband (UWB). While WAN is a regional backbone, part of a high-use network, and LAN/WLAN is mainly used for file-sharing and Internet access routing, the use of a PAN can be divided into either lower data rate systems such as mobile phone for access to larger systems or high rate data systems such as household video or audio distribution.

### 3. Motivations

Apart from one or more local interfaces for intra-PAN communication, however, a PAN component may also have a global network interface for inter-PAN communication to enable access to other networks, such as other PANs or the Internet. Two or more PAN users can meet and form a community area network (CAN), or multiple PAN users can interconnect with the aid of wireless mesh networks (WMNs) [4]. In wireless mesh networks, multihop ad hoc networks are not isolated self-configured networks, but act as a flexible and low-cost extension of wired infrastructure networks, employing multihop communications to forward traffic en route to and from a wired Internet entry point. With the aid of WMNs, PANs can transparently and conveniently connect to much larger networks, as shown in the Figure 1. The design of a future key management scheme for PANs should thus take this environment into account in order to facilitate mass market deployment of PANs. Thus, security issues in the inter-PAN environment must also be considered.

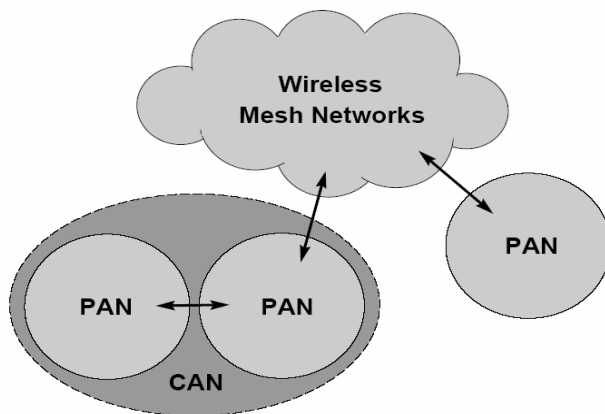


Figure 1. An inter-PAN communication scenario

#### 3.1 Wireless mesh networks (WMNs)

Despite much effort in researching and developing mobile ad hoc networks (MANETs) over the last decade, MANET technology has not yet had much effect on the use of wireless communication by the general population. Much previous work has focused on implementing military or specialised civilian applications. Proposed key management schemes for MANETs suffer from the main constraint of MANETs —no pre-existing communications infrastructure.

A new class of network is now emerging, designed to turn

MANETs into a commodity: wireless mesh networks (WMNs) [4]. In wireless mesh networks, multihop ad hoc networks are not isolated self-configured networks, but act as a flexible and low-cost extension of wired infrastructure networks, employing multihop communications to forward traffic en route to and from a wired Internet entry point. With the aid of WMNs, PANs will be able to transparently and conveniently connect to much larger networks. The design of a future key management scheme for PANs should thus take this environment into account in order to facilitate mass market deployment of PANs.

#### 3.2 Previous solutions

A security association between devices within a PAN typically incorporates shared secrets and/or trusted public keys. An initial secure channel can be used to create a security association between devices, and this association can then be used to perform authenticated key establishment whenever necessary. Providing key pre-distribution in PANs remains a challenging problem, in particular because of the unique characteristics of, and constraints on, such networks. Several key pre-distribution schemes have been proposed for use in PANs (see, for example [10]-[13], [19]), but these schemes only address security issues for intra-PAN communication. These solutions could be divided into symmetric-key solutions known as manual authentication techniques [11], [12] and public-key solutions designed to reliably exchange public keys, namely certificate-based [13], [19] and identity-based models [10].

#### 3.3 ID-based cryptography

Symmetric solutions such as manual authentications [11], [12] are attractive in terms of efficiency in closed small networks, but may be not appropriate for potentially dynamic and large networks; whenever a new device join the network, it should perform the manual authentications with all existing network nodes.

As public-key solutions, ID-based schemes have certain efficiency advantages for securing mobile ad hoc networks as well as personal area networks when compared to conventional certificate-based schemes, as shown in [6], [10]. We note, however, two main drawbacks of ID-based schemes: (1) a private key generator (PKG) has knowledge of all the device private keys; and (2) a secure channel between a PKG and each network device is required for the secure distribution of private keys.

The proposed scheme eliminates the first issue by taking advantage of the unique characteristics of a PAN. We propose that one device from each PAN, which we call a *distributed private key generator (DPKG)*, performs private key generation on behalf of devices within a PAN. Of course, this approach does not match the original goal of DPKGs, since the chosen DPKG can impersonate any of the PAN devices using knowledge of its private key. However, devices within the same PAN can be assumed to trust each other, since all devices within a PAN are owned and controlled by a single user. The latter problem can be efficiently solved using techniques from [10]-[11], [24].

### 3.4 Application of threshold cryptography

It is problematic to provide a key management service using a single PKG in an ad hoc network; the PKG could be a point of vulnerability in the network. Moreover, if the PKG is unavailable, the nodes cannot establish secure communication. However, a naïve replication of PKG functionality to address availability could make the service more vulnerable; if one PKG is compromised, then the private keys of all network nodes can be recovered, rendering all communications insecure. To solve this problem, we distribute trust to a set of nodes by letting these nodes share the key management responsibility.

Specifically, we propose that the participating PAN users generate cryptographic keys in a distributed fashion. Distribution of trust in our key management service is accomplished using threshold cryptography. In a  $t$ -out-of- $n$  threshold scheme, any set of  $t$  parties can jointly perform cryptographic operations, while it is infeasible for fewer than  $t$  parties to do so. Therefore, by employing an  $(n, t)$ -threshold scheme, we can split a master secret  $s$  into  $n$  shares  $s_1, s_2, \dots, s_n$  and distribute one share to each DPKG.

## 4. Proposed Scheme

### 4.1 Cryptographic assumptions

Most schemes based on ID-based cryptography employ bilinear pairings. A bilinear map,  $e: G_1 \times G_2 \rightarrow G_T$  for additive groups  $G_1, G_2$  and multiplicative group  $G_T$  of prime order  $q$ , satisfies the following properties:

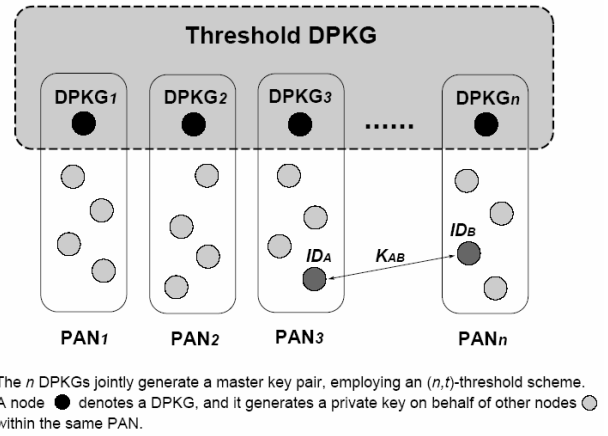
- *Bilinearity*:<sup>2</sup>  $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$  for all  $g_1 \in G_1$ ,  $g_2 \in G_2$ , and  $a, b \in \mathbf{Z}_q$ .
- *Non-degeneracy*:  $e(g_1, g_2) \neq 1$  for some  $g_1 \in G_1$  and  $g_2 \in G_2$ .
- *Computability*:  $e(\cdot, \cdot)$  is efficiently computable.

In our scheme, we set  $G_1 = G_2$  for simplicity.

### 4.2 Setup and Secret Sharing

Our network scenario involves a limited number of people with multiple wireless personal devices who wish to form an ad hoc network to share important information. We first point out that all self-organising key distribution schemes require some kind of *a priori* security association between the participating communication entities, i.e. it is not possible to create trust from scratch.

<sup>2</sup> Instead of the additive notation used in elliptic curve settings, we use multiplicative group notation for the pairing.



**Figure 2.** A threshold DPKG for intra/inter-PAN communication

We assume each DPKG from PANs has a secure channel with either a trusted authority (TA). These devices<sup>3</sup> function as DPKGs employing a  $t$ -out-of- $n$  threshold scheme, receiving a share of a system master secret from the TA, using the techniques described in [9]. They generate the private keys for other PAN devices in a distributed fashion.

If PAN users want to generate a master secret without a trusted authority, the  $n$  DPKGs are also able to jointly generate a master secret, using the protocol from [14], at the cost of greater computation and communication complexity. In this case, in order to implement the secret sharing scheme, secure channels are only required between the  $n$  DPKGs instead of between all network nodes.

We suggest that all the devices from the  $n$  participating PANs using the ID-based threshold scheme should employ the same set of ID-based parameters, and then any two entities from different PANs will be able to generate public keys for one another using a single set of domain parameters.

#### 4.2.1 Setup with TA

**Setup** The TA chooses two groups  $G_1$  and  $G_2$  of the same prime order  $q$ , where the Discrete Logarithm Problem (DLP) is computationally infeasible in both groups. In practice, the group  $G_1$  could, for example, be a subgroup of the additive group of points of an elliptic curve  $E/F_p$ , and  $G_2$  a subgroup of the multiplicative group of a finite field  $F_p^*$ . The TA also chooses an admissible bilinear map  $e: G_1 \times G_1 \rightarrow G_2$  and a hash function  $H: \{0,1\}^* \rightarrow G_1^*$ , as described in [2], and selects the system master secret  $s \in \mathbf{Z}_q^*$ .

To distribute a master secret  $s$  among  $n$  DPKGs, a TA chooses a polynomial  $f(z) = \sum_{k=0}^{t-1} a_k z^k \in \mathbf{Z}_q[z]$  of degree at most  $t-1$  such that  $f(0) = a_0 (= s)$ . The TA computes

<sup>3</sup> We assume that DPKGs are physically secure, are computationally more powerful than other PAN devices, and also have communication channels to other PANs. A DPKG can then function as a gateway to other PANs for inter-PAN communications.

DPKG<sub>*i*</sub>'s share  $s_i$  as  $f(ID_i) = s_i (1 \leq i \leq n)$  and then securely transfers  $s_i$  to DPKG<sub>*i*</sub>, where an  $ID_i$  is a unique identifier of a DPKG<sub>*i*</sub>.

**Verification of setup** Any group of  $t$  DPKGs can recover the secret  $s$  using the Lagrange interpolation formula. Feldman's *Verifiable Secret Sharing* (VSS) scheme [9] allows each DPKG to validate the correctness of the received shares; the TA computes a commitment to the coefficient  $a_i$  ( $i = 0, 1, \dots, t-1$ ) in the form of a witness  $w_i = g^{a_i} \bmod p$ , where  $g \in \mathbf{Z}_p^*$  has order  $q$  such that  $q | (p-1)$ . The secret share  $s_i$  can be validated by checking the following equation;

$$g^{s_i} = \prod_{k=0}^{t-1} (w_k)^{ID_i^k} \bmod p.$$

The parameters  $\langle p, q, e, G_1, G_2, g, w_i \rangle$  are published in an online trusted public repository or preloaded to each DPKG, while  $s$  should never be disclosed.

**Secure channel establishment between DPKGs** Secure channels between DPKGs can be established in a non-interactive fashion using  $(s_i, g^{s_i})$  as a private/public key pair for each DPKG, as in [23]. The public key  $g^{s_i}$  can readily be computed by any network node using the public parameters and the unique identifier  $ID_i$ . Any pair of DPKGs, DPKG<sub>*i*</sub> and DPKG<sub>*j*</sub>, say, can establish a shared secret key as follows:

$$K_{ij} = (g^{s_j})^{s_i} \bmod p = (g^{s_i})^{s_j} \bmod p = K_{ji} \quad (1)$$

The use of  $(s_i, g^{s_i})$  as private/public key pair seems attractive as a key management model for MANETs. However, given that the MANETs are likely to have a dynamic membership, the scheme becomes less attractive when nodes join and/or leave the network, since this may mean that all nodes will need to change their private/public key pairs. In our scheme, we use these key pairs only to facilitate non-interactive secure channel establishment, and actual private keys of DPKGs can be generated as below.

Using secret shares as private keys can be viewed as an ID-based cryptosystem with the additional assumption that the threshold number of nodes has not been compromised. This is because a node can send an encrypted message and verify signatures with the knowledge of the identifier of a particular node and the public system parameters. However, unlike other ID-based schemes, the security of the scheme is based on the standard Discrete Logarithm Problem (DLP), and the scheme becomes insecure once more than  $t-1$  DPKGs have been compromised.

#### 4.2.2 Setup without TA

The  $n$  DPKGs choose two groups  $G_1$  and  $G_2$ , as described in the previous section 4.2.1. The DPKGs also choose an admissible bilinear map  $e: G_1 \times G_1 \rightarrow G_2$  and a hash function  $H: \{0,1\}^* \rightarrow G_1^*$  as described in [2]. The DPKGs then choose

a master secret and distribute it verifiably among themselves without relying on a trusted party<sup>4</sup>. More specifically, each DPKG<sub>*i*</sub> ( $1 \leq i \leq n$ ) randomly chooses  $x_i = \mathbf{Z}_q$  and a polynomial  $f_i(z) \in \mathbf{Z}_q[z]$  of degree at most  $t-1$  such that  $f_i(0) = x_i$ . After computing  $s_{ij} = f_i(j)$  for  $j = 1, 2, \dots, n$ , DPKG<sub>*i*</sub> sends  $s_{ij}$  to DPKG<sub>*j*</sub> via a secure channel, reserving  $s_{ii}$  for itself. Finally, DPKG<sub>*i*</sub> computes its share of the master secret  $s = \sum_{k=1}^n x_k \bmod q$  as

$$s_i = \sum_{j=1}^n s_{ji} \bmod q.$$

If we define the polynomial  $f(z) = f_1(z) + f_2(z) + \dots + f_n(z) \in \mathbf{Z}_q[z]$ , it is easy to check that  $s_i = f(i)$  for every  $i = 1, 2, \dots, n$ , and thus  $s_i$  is a share for the polynomial  $f$ . More detailed discussions of share verification and realising a uniform distribution of keys can be found in [14]. The verification of setup process is the same as in section 4.2.1.

#### 4.3 Private key generation

As mentioned previously, a DPKG performs private key generation on behalf of devices within a PAN, including itself, which potentially increases efficiency without decreasing the level of security. For a node to receive the private key,  $d_{ID}$ , corresponding to its identity,  $ID$ , a node presents its identity and any information specified by the key issuance policy to the DPKG within the same PAN, and the DPKG relays the information to  $t-1$  (or more<sup>5</sup>) other DPKG nodes: DPKG<sub>*i*</sub>, DPKG<sub>*i*</sub>, ..., DPKG<sub>*i*</sub>, say. We note that the DPKG node could also generate one of private key shares itself. It then receives in return key shares  $d_{ID}^{i_j} = s_{i_j} Q_{ID} (\in G_1)$  via secure channels, where  $Q_{ID} = H(ID)$  is the node's public key, and can compute the private key  $d_{ID}$  as

$$d_{ID} = \sum_{j=1}^t \lambda_j d_{ID}^{i_j} (\in G_1)$$

from the  $t$  shares, where the values  $\lambda_j$  are the appropriate Lagrange coefficients. We note that the Lagrange coefficients above are assumed to be public values. Further techniques for enhancing the robustness of private key generation are discussed in [2]. Once a private key has been computed by a DPKG, it must be securely transferred to the appropriate mobile device.

#### 4.4 Secure transfer of private keys

This secure channel must provide data origin authentication as well as confidentiality. Such a channel can be established with

<sup>4</sup> We describe a basic verifiable secret sharing scheme, as proposed by Pedersen [21]; Gennaro et al. [14] have developed this scheme to enable it to resist various attacks.

<sup>5</sup> Due to the error-prone nature of wireless links, use of greater than  $t-1$  other DPKGs will reduce the risk of a DPKG not receiving enough shares of a private key.

the aid of manual authentication techniques, as described in [10]-[11], or visual channels [24].

Manual authentication protocols [11]-[12] require the devices to possess human interfaces such as a key pad and display. Since the PAN components are close to each other and there is, in most cases, at least one human that controls the components, a secure channel can be established with the assistance of the human. A human operator could be asked to copy data from one device into another, compare the output of two devices, or enter the same data into both devices. With the aid of the manual transfer of data, PAN devices can be imprinted with the necessary security association via an insecure wireless channel. A variety of such protocols exist, with varying requirements on the display and input capabilities of the devices.

We show one of manual authentication protocols for the secure channel establishment within PANs. A group  $G$ , in which the Diffie-Hellman problem is intractable, and an element  $g \in G$  are chosen so that  $g$  generates a large subgroup of  $G$  of prime order. We assume that the DPKG and all the PAN devices share a suitable MAC function (see [11]). The following authenticated Diffie-Hellman exchange protocol can be used, where a PAN device  $D$  and a DPKG within the same PAN establish a shared secret key in order to establish a secure channel.

- (1) The DPKG generates a random integer  $x$  and sends  $g^x$  to the device  $D$ .
- (2) The device  $D$  generates a random integer  $y$  and sends  $g^y$  to the DPKG.
- (3) The DPKG generates a random key  $K$  which is suitable for a MAC function.
- (4) The DPKG computes  $\text{MAC}_K(g^x, g^y)$  which is output along with the key  $K$  via the display of the DPKG.
- (5) The user then types the key  $K$  and the MAC value into the device  $D$ , and  $D$  checks the MAC value with input  $g^x, g^y$  and key  $K$ .
- (6) If the two values match, then both  $D$  and the DPKG generate  $g^{xy}$  as a shared secret.

#### 4.5 Beyond bootstrapping security

Although we aim to establish a shared secret key between any two devices, ID-based signature schemes based on elliptic curve cryptography can be used whenever necessary with assigned private/public key pairs for each node, e.g., to provide a non-repudiation service. An ID-based signature scheme such as that described in [5] yields signatures that are both very efficient to compute and extremely short (roughly 160 bits long).

We, however, do not expect that most PAN devices are capable of performing public-key cryptography; at most efficient symmetric-key cryptography may be applicable. In fact, shared secrets can be established between any network node in a non-interactive fashion, form the result of bootstrapping security. Any two network nodes, with identifiers  $ID_A$  and  $ID_B$ , can establish a shared secret key

$K_{AB} (= K_{BA})$  in a non-interactive fashion, as follows [22]:

$$K_{AB} = e(d_A, Q_B) = e(d_B, Q_A) = K_{BA}, \quad (2)$$

where  $e(\cdot)$  is a bilinear mapping, and  $d_i$  and  $Q_i$  are the private/public keys respectively of the network node with identifier  $ID_i$ . In fact, they only need to compute  $K_{AB}$  once and cache the result, obviating an expensive pairing computation, which makes the system as efficient as a symmetric cipher. We illustrate the specific protocols of using shared secrets for secure data communications in the section 7.

## 5. Analysis

### 5.1 Security analysis

We have proposed two different non-interactive key establishment methods for use during the initialisation phase in our inter-PAN environment. These keys can be used as long-term shared secrets between each pair of parties. Then these keys must be guaranteed to be secure enough for subsequent key agreement protocols. Boyd, Mao and Paterson [3] describe provably secure key agreement schemes with a MAC-based authenticator, using two different long-term static keys; a static Diffie-Hellman key,  $K_{ij}$  from (1), and an identity-based static key,  $K_{AB}$  from (2). The security of a MAC-based authenticator using a Diffie-Hellman static key  $K_{ij}$  relies on the difficulty of the Computational Diffie-Hellman Problem (CDHP) in  $\mathbf{Z}_p^*$ , i.e. given  $g, g^x, g^y$  in  $\mathbf{Z}_p^*$  with  $x, y \in \mathbf{Z}_q$ , compute  $g^{xy} \in \mathbf{Z}_p^*$ . Similarly, the security of a MAC-based authenticator using an identity-based static key  $K_{AB}$  depends on the hardness of the Bilinear Diffie-Hellman Problem (BDHP) in  $\langle G_1, G_2, e \rangle$ , i.e. given  $(P, xP, yP, zP)$  with  $P \in G_1$  and  $x, y, z \in \mathbf{Z}_q$ , compute  $e(P, P)^{xyz} \in G_2$ . Using the above assumptions, the security of a MAC-based authenticator can be proven by replacing the MAC with a hash function, where the static key is included as an input to the hash, and modelling the hash function as a random oracle.

### 5.2 Efficiency analysis

**Efficiency from hierarchical structure** Our model is a hierarchical structure, as shown in the Figure 2. We assume that one device within each PAN is physically secure and computationally more powerful than other PAN devices, and also have reliable communication channels to other PANs. These devices comprise DPKGs, performing as gateways for each PAN.

By delegating the private key generation process for other personal wireless devices, which may have limited resources, to a PAN gateway, we decrease both the computations and communications such personal devices need to perform. That is, a PAN device will only need to contact its gateway instead of communicating with  $t$  DPKGs for private key generation; if all network nodes function as DPKGs, personal wireless devices, which generally have a local communication interface

with limited capacity, will not necessarily be able to connect to as many as  $t$  DPKGs in order to get the necessary private key shares. This greatly improves communication efficiency, because wireless transmission of a bit can require over 1,000 times more energy than a single 32-bit computation [18].<sup>6</sup> Moreover, secure channels for the transfer of private key shares are only required between DPKGs, rather than between DPKGs and all devices, as required by previous schemes for MANETs.

**Efficiency over certificate-based scheme** Manual key pre-distribution schemes based on symmetric cryptography [10]-[11], [24] are not appropriate as the network size increases; for example, manual pairing process needs to be performed  $n(n-1)/2$  times for  $n$  network devices. Public-key based solutions are thus more efficient for large networks with dynamic membership. As an alternative key pre-distribution scheme for the inter-PAN environment, we might also consider a certificate-based threshold scheme.

The concept of a personal PKI [13], [19] was introduced for use in a PAN with motivations; (1) users who want to manage their own local environments, such as PANs, will gain few benefits from employing a centralised CA, and (2) users might not want to delegate CA operations to an external CA for privacy reasons. The scheme operates somewhat differently to a large scale PKI. One of the PAN devices must act as a personal CA, and issue and distribute certificates for the other PAN devices. The public key in the certificates can then be used to authenticate PAN devices to one another or establish session keys between devices. Personal CAs, one from each PAN, may form a distributed CA, and jointly sign certificates for devices in PANs, using the technique described by Zhou and Haas [26]. This scheme can be applied where an ID-based scheme is not applicable or the use of certificates is preferred.

ID-based schemes, however, have certain efficiency advantages in terms of computation and communication based on equivalent security level for securing personal area networks when compared to conventional certificate-based schemes, as shown in [10]. Moreover, [17] discuss that distributed PKG is also more efficient than distributed CA. Public keys in ID-based schemes are self-authenticating, hence certificates are not required, and the need to generate public keys and distribute them throughout the network in advance is avoided. Identities, such as IP and/or MAC addresses, can be propagated in transmitted messages. Thus, ID-based schemes reduce the computation necessary to join the network, and also potentially lead to savings in bandwidth.

## 6. Other discussion

### 6.1 DPKG failure and pinpoint attack

The proposed scheme is both resilient to failures of one or more DPKGs, and tolerant to faulty or malicious behaviour by

<sup>6</sup> Transmitting a sufficiently powerful signal, or decoding a received spread-spectrum signal, involves considerable energy consumption, equivalent to that used by several thousand cycles of the CPU. See, e.g., <http://xbow.com>

up to  $t-1$  DPKGs. However, a DPKG in a PAN is a single point of failure for the communications of the other devices within the PAN. In the event of a DPKG failure, the next most computationally powerful and secure device within the PAN can be used to replace the original DPKG, using share refreshing techniques [16]. The shared communication medium allows adversaries to easily locate DPKGs by eavesdropping on IDs sent in data packets. An adversary could then launch an attack to disrupt the functionality of a target DPKG. This can be prevented by use of the MASK [25] routing protocol, which uses dynamically changing pseudonyms in the routing process without disclosing the real identities of packet sources and destinations and all the intermediate nodes.

### 6.2 Sharing updating and handling new DPKGs

When we apply threshold cryptography, the scheme needs to tolerate mobile adversaries and to adapt its configuration to changes in the network. Ostrovsky and Yung [20] first introduced the notion of mobile adversaries, i.e. adversaries which temporarily compromise one server and then move on to the next victim, eventually compromising all servers over a long period of time. As a countermeasure to mobile adversaries, proactive schemes [16] can be used, where share refreshing enables servers to update new shares from old ones without changing the system master secret. To accommodate DPKGs joining and leaving, any necessary changes of configuration, such as from an  $(n,t)$  to an  $(n',t')$ -threshold scheme, can be managed by share refreshing. However, secret sharing parameters  $t,n$  need to be chosen to achieve a good trade-off between security and robustness. In particular, for a fixed  $n$ , a larger  $t$  means that adversaries need to compromise more DPKGs (*more secure*), but they only need to disrupt fewer DPKGs (*less robust*). It is often suggested to let  $t = \lceil n/2 \rceil$ , and a more detailed discussion on the selection of the secret share parameters in ad hoc environments can be found in [18].

### 6.3 Key update and revocation

Key update and revocation are also important issues in an ID-based key management scheme. In fact, it is not sufficient to associate an expiry date with a public key to support key revocation, since keys in malicious or compromised devices may need to be revoked prior to expiry. Devices also need to be able to request key renewal in the case of key compromise. However, these topics are outside the scope of this paper; an elegant discussion of key update and revocation issues in ID-based key management scheme in MANETs appears in [18].

### 6.4 Generalisation

Even though we proposed the key pre-distribution scheme for inter-PAN environment, the proposed scheme may be applied to any network environment with the following properties; (1) the network consists of small independent networks, and (2) a certain degree of trust exists between all network nodes within

each individual network. The proposed scheme, for example, may be applied to secure communications in military tactics, where the network consists of several platoons.

## 7. Data Communication Security in PANs

The proposed scheme provides every pair of nodes in the network with a pre-shared secret. In this section, we briefly consider how these pre-shared secrets can be used to support transport layer security in order to secure personal area networks.

Although all security services could be provided at the link layer, link layer security cannot provide end-to-end secure communication. Moreover, because it is expected that future personal mobile devices will be capable of running a generic transport protocol, it would be natural to perform authentication of the devices and to secure data communication at the transport layer.

Transport layer security (TLS) [7] could be deployed in a PAN in order to provide connection security with peer entity authentication, data confidentiality and integrity, key generation and distribution, and cryptographic parameter negotiation. Although schemes for a version of TLS optimised for wireless communications have been proposed, such as WTLS within WAP [1], wireless environments were not considered at the initial design stage of the TLS protocol. While the security of future mobile systems beyond the third generation are expected to be supported by a PKI, implementing full PKI support in constrained devices with reduced networking and processing capabilities appears difficult.

A number of authors have considered how TLS might be modified to use shared secrets, especially in mobile environments. These methods typically avoid expensive public-key operations involving certificates in the TLS handshake, while providing an equivalent level of security using shared secret keys. Gutmann [15] suggests seeding the TLS session cache with the shared key and using session resumption functionality without changing the TLS protocol. In this scheme, prior to any exchange, the client and server session caches are seeded with a session ID identifying the user/session, and a master secret derived from the shared secret keys. Eronen and Tschofenig [8] propose three sets of new ciphersuites for the TLS protocol to support authentication based on a pre-shared secret. In particular, the first set of ciphersuites uses only symmetric algorithms and is thus suited to performance-constrained devices.

## 8. Related Work

ID-based schemes potentially provide more efficient security frameworks than conventional PKIs in PANs and MANETs, as we will discuss in the next section, and the application of threshold cryptography addresses a key management issue in a distributed environment. As a result, ID-based threshold schemes have been proposed to support key pre-distribution for MANETs [6], [17]. These schemes involve the application of ID-based threshold schemes to mobile ad hoc networks, in

which it is assumed that a trusted party such as an external PKG is not available. When the nodes decide to form a network, they agree on a mutually acceptable set of security parameters such as a threshold  $t$ , key lengths, and/or a key issuance policy. The initial set of  $n$  nodes then act as distributed PKGs (DPKGs), employing an  $(n, t)$ -threshold scheme. A system master secret can be jointly generated by the DPKG without a trusted party using techniques described in [14], so that the master secret is not stored or computed in any single location. The DPKGs can then offer a collaborative private key generation service for other network nodes, including themselves; such an approach also efficiently eliminates the key escrow issue of ID-based schemes.

Khalili, Katz and Arbaugh [17] assume that there is no prior shared keying material or trust/security association between DPKGs, and instead attempt to establish these at the time of network formation. However, all the verifiable secret sharing schemes without a trusted third party known to the author require secure channels between all network nodes for the distribution of master secret shares. We also note that they do not address the issue of protecting the confidentiality and integrity of the private key shares when transferred from the DPKGs to the mobile device. Providing such a secure channel is a non-trivial problem. To address this issue, Deng and Agrawal [6] propose that each DPKG encrypts the share using a requesting mobile device's temporary public key. Since this temporary public key is not certified, the adversary can spoof the public key of the requesting device, and then recover the distributed private key by combining decrypted private key shares.

These existing schemes use key pre-distribution frameworks to provide security associations, which can be used for subsequent authenticated key establishment. However, they implicitly assume that all nodes already have trusted copies of public keys of other nodes, or they have pairwise shared secret keys, either to perform a secret sharing scheme or to securely transfer secret shares of each node's private key.

## 9. Conclusion

Personal wireless devices are usually resource-constrained devices. The self-organising property of a PAN environment also makes bootstrapping security a challenging task. We thus propose an effective and robust self-organising key pre-distribution protocol for intra/inter-PAN environments. Using the proposed scheme, any two devices can establish a shared secret in a non-interactive fashion, which makes ad hoc routing protocols and subsequent authenticated key establishment extremely efficient. The shared secrets can then be used to support end-to-end communication security for PANs using only symmetric algorithms.

## References

- [1] P. Ashley, H. M. Hinton, and M. Vandenwauver. "Wired versus wireless security: The Internet, WAP and iMode for E-Commerce", In *Proceedings of 17th Annual*

- Computer Security Applications Conference (ACSAC 2001)*, pp. 296-308, 2001.
- [2] D. Boneh and M. K. Franklin. "Identity-based encryption from the Weil pairing", In *Proceedings of 21st Annual International Cryptology Conference (CRYPTO 2001)*, pp. 213-229, 2001.
- [3] C. Boyd, W. Mao and K. G. Paterson. "Key agreement using statically keyed authenticators", In *proceedings of 2th International Conference on Applied Cryptography and Network Security (ACNS'04)*, pp. 287-305, 2004.
- [4] R. Bruno, M. Conti and E. Gregori, "Mesh networks: commodity multihop ad hoc networks", *IEEE Communications Magazine*, 43(3), pp. 123-131, 2005.
- [5] J. Cha and J. Cheon, "An identity-based signature from Gap Diffie-Hellman groups", In *proceedings of 6th International Workshop on Theory and Practice in Public Key Cryptography: Public Key Cryptography*, pp. 18-30, 2003.
- [6] H. Deng and D. P. Agrawal, "TIDS: Threshold and identity-based security scheme for wireless ad hoc networks", *Ad Hoc Networks*, 2(3), pp. 291-307, 2004.
- [7] T. Dierks and E. Rescorla, "The TLS Protocol Version 1.1", *IETF Internet Draft*, March 2003.
- [8] P. Eronen and H. Tschofenig, "Pre-shared key ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.
- [9] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", In *28th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 427-437, IEEE, 1987.
- [10] T. Garefalakis and C. J. Mitchell, "Securing Personal Area Networks", In *Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2002)*, pp. 1257-1259, IEEE, 2002.
- [11] C. Gehrman and C. J. Mitchell and K. Nyberg, "Manual Authentication for Wireless Devices", *Cryptobytes*, 7(1), pp. 29-37, Spring 2004.
- [12] C. Gehrman and K. Nyberg, "Security in personal area networks", In *Security for Mobility*, C. J. Mitchell (eds.), IEE, London, 2004.
- [13] C. Gehrman, K. Nyberg and C. Mitchell, "The personal CA - PKI for a Personal Area Network", In *Proceedings of IST Mobile & Wireless Communications Summit 2002*, pp. 31-35, 2002.
- [14] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystem", In *proceedings of International Conference on the Theory and Application of Cryptographic Techniques (Eurocrypt 99)*, pp. 295-310, Springer, 1999.
- [15] P. Gutmann, "Use of Shared Keys in the TLS Protocol", Internet draft (expired), draft-ietf-tls-sharedkeys-02, October 2003.
- [16] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage", In *proceedings of the 15th Annual International Cryptology Conference (CRYPTO '95)*, volume 963 of LNCS, pp. 339-352, Springer, 1995.
- [17] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks", In *Proceedings of IEEE Security and Assurance in Ad-Hoc Networks at Int'l Symposium on Applications and the Internet (SAINT '03)*, pp. 342-346, IEEE, 2003.
- [18] W. Liu, Y. Zhang, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public Keys", *IEEE Transactions on Dependable and Secure Computing*, 3(4), pp. 386-399, 2006.
- [19] C. J. Mitchell and R. Schaffelhofer, "The personal PKI", In *Security for Mobility*, C. J. Mitchell (eds.), IEE, London, 2004.
- [20] R. Ostrovsky and M. Yung, "How to withstand mobile virus attacks", In *Proceedings of the 10th Annual Symposium on Principles of Distributed Computing (PODC '91)*, pp. 51-59, 1991.
- [21] T. P. Pedersen, "A threshold cryptosystem without a trusted party (Extended Abstract)", In *Eurocrypt '91*, pp. 522-526, 1991.
- [22] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing", In *the 2000 Symposium on Cryptography and Information Security (SCIS '00)*, pp. 26-28, January 2000.
- [23] N. Saxena, "Public key cryptography sans certificates in ad hoc networks", In *Proceedings of 4th International Conference on Applied Cryptography and Network Security (ACNS'06)*, volume 3989 of LNCS, pp. 375-389, 2006.
- [24] N. Saxena, J. Ekberg, K. Kostiaainen, and N. Asokan, "Secure device pairing based on a visual channel (short paper)", In *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P '06)*, pp. 306-313, IEEE Computer Society, 2006.
- [25] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Anonymous communications in mobile ad hoc networks", In *Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005)*, pp. 1940-1951, IEEE, 2005.
- [26] L. Zhou and Z. J. Haas, "Securing ad hoc networks", *IEEE Network*, 13(6), pp. 24-30, 1999.

## Author Biography

**Jihoon Cho** received a BSc in Mathematics from Kyungpook National University (South Korea). He then joined the Department of C&O (CACR), University of Waterloo, Canada, specialising in public-key cryptography. He subsequently completed an MSc in Information Security at Royal Holloway, and joined the ISG PhD programme in 2005. His research interests include security and privacy issues in ubiquitous computing environment.